Amendments to the CLAIMS

1. (currently amended) A security device comprising:

a memory device comprising:

a first memory portion configured to store a device ID; ~~and~~

a second memory portion configured to store a device secret; and

a third memory portion configured to store a service provider data item;

a processor connected to the memory device, the processor configured to read the stored device ID from the first memory portion ~~and~~, the stored device secret from the second memory portion, and the stored service provider data item from the third memory portion, and to perform a nonreversible computation using the stored device ID, the stored device secret, the stored service provider data item, and a challenge as seeds; and

a communication circuit connected to the processor, the communication circuit configured to receive the challenge from a host device and to communicate a result of the nonreversible computation performed by the processor.

2. (canceled)

3. (original) The security device of claim 2, wherein the memory device further comprises:

a fourth memory portion configured to store a counter value that is incremented responsive to the service provider data item being changed;

wherein the stored counter value is also used to seed the nonreversible computation.

4. (original) The security device of claim 1, wherein the first memory portion comprises a nonvolatile and unalterable memory device.

5. (original) The security device of claim 4, wherein the second memory portion comprises an unalterable memory portion.

6. (cancelled)

7. (original) The security device of claim 1, wherein the security device is incorporated into a smart card.

8. (canceled)

9. (original) The security device of claim 1, wherein the security device is incorporated into a host device.

10. (original) The security device of claim 1, wherein the nonreversible computation is a SHA-1 computation.

11. (original) The security device of claim 10, wherein the processor is configured to perform the SHA-1 computation serially.

12. (original) The security device of claim 10, wherein the processor is configured to perform the SHA-1 computation in parallel.

13. - 16. (canceled)

17. (currently amended) The method of claim 34 ~~15~~, further comprising the step of:

enabling an electronic device responsive to a positive authentication of the roaming device ~~received response~~.

18. (currently amended) The method of claim 34 ~~15~~, further comprising the step of:

disabling an electronic device responsive to a failure to authenticate the roaming device ~~the received response~~.

19. (currently amended) A system for device authentication, the system comprising:

a coprocessor security device configured to store a service provider data item and a device secret; and

a host device connected to the coprocessor security device, the host device configured to communicate with the coprocessor security device and a roaming security device, the roaming security device being configured to store a plurality of different service provider data items such that said roaming security device may communicate with a plurality of different service providers;

wherein the roaming security device can be authenticated to thereby enable the host device.

20. (original) The system of claim 19, further comprising:

a printer, wherein the coprocessor security device is attached to the printer.

21. (original) The system of claim 19, further comprising a means for attaching the roaming security device to a printer cartridge.

22. (original) The system of claim 19, further comprising:

a means for attaching the roaming security device to a printer.

23. (original) The system of claim 20, wherein the printer cartridge is disabled responsive to the roaming security device being removed from the printer cartridge.

24. (currently amended) A method of device authentication, the method comprising the steps of:

receiving, at a roaming device, a challenge from a host device;

generating, at the roaming device, a first nonreversible computation result, wherein the first nonreversible computation result is computed by seeding a first nonreversible algorithm with at least the challenge, a selected service provider data item, and a roaming device secret; ~~and~~

outputting to the host device a response to the challenge, wherein the outputted response includes the first nonreversible computation result,

outputting to the host an identification and at least another data item including one of a plurality of service provider data items;

generating, at the host device a second nonreversible computation result, wherein the second nonreversible computation result is computed by seeding a second nonreversible algorithm with at least a challenge, said selected service provider data item and a host device secret;

comparing, by said host device, said first nonreversible computation and said second nonreversible computation in order to authenticate the roaming device.

25. - 26. (canceled)

27. (currently amended) The method of claim 24, further comprising ~~the step of~~:

enabling an electronic device responsive to a positive authentication of the ~~received response~~ roaming device.

28. (currently amended) The method of claim 24, further comprising ~~the step of~~:

disabling an electronic device responsive to a failure to authenticate the roaming device ~~received response~~.

29. (currently amended) The method of claim 24, wherein the first nonreversible computation result is computed by further seeding the first nonreversible algorithm with a unique device identifier.

30. - 33. (canceled)

34. (new) A method of device authentication for a plurality of service providers comprising the steps of:

receiving, by a roaming device, a challenge from a device;

generating, by said roaming device, a first nonreversible computation result;

outputting, by said roaming device to said device, a response to the challenge, wherein the outputted response includes the first nonreversible computation result; wherein the first nonreversible computation result is computed by seeding an algorithm with the received challenge, a secret known by said roaming device and said device, a unique roaming device identifier and one of a plurality of service provider identifiers;

reading, by said device from said roaming device, at least said unique roaming device identifier;

generating, by said device, a second nonreversible computation result, wherein said second nonreversible computational result is computed by seeding a second algorithm with said challenge, said secret known by said roaming device and said device, said one of a plurality of service provider identifiers and said unique roaming device identifier read from said roaming device; and

comparing said first nonreversible computational result with said second nonreversible computational result in order to authenticate said roaming device for a selected one of a plurality of service providers.